IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
STEPHEN G. PERLMAN	Examiner: Mills, Donald L.
Serial No.: 10/618,931	Art Unit: 2416
Filing Date: July 14, 2003	Confirmation No.: 6609
For: **SELF-CONFIGURING, ADAPTIVE, THREE-DIMENSIONAL, WIRELESS NETWORK**	

Declaration Under 37 C.F.R. § 1.132

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

I, Stephen G. Perlman, declare that:

1. I received a Bachelor of Arts Degree from Columbia University in 1983. As an engineer and a pioneering innovator in the entertainment, multimedia, computer, communications, and consumer electronics technological fields I am completely self-taught. I received a ham radio license in junior high school; built my first computer at age 16; designed and built my own color graphics display at age 17; and designed and built a novel software-based state-of-the-art 1200 bps modem in 1980 at age 19, which cost only $25 to build, at a time when commercially-available 1200bps modems were hardware-based and sold for over $1000.

2. In 1985 I joined Apple Computer, Inc. where I became a Principal Scientist.

My team was responsible for the development of the underlying multimedia (color graphics, sound, 3D, animation, displays, and video) technology incorporated into the color Macintosh computer, including the underpinnings of the present-day QuickTime® technology. To this day, all Macintosh computers, iPhones and video iPods are still utilizing these technologies, and QuickTime is used in a large percentage of PCs as well. After several years, I left Apple to work as Managing Director of Advanced Products for General Magic developing a software modem technology, later acquired by Broadcom, and system-on-a-chip with an embedded MIPs CPU modified with DSP capability that was manufactured by Sony, IDT and Philips and became the core silicon for the first WinCE PDAs; then later, in 1994, I co-founded Catapult Entertainment. As Catapult's Chief Technology Officer I was responsible for the design and development of proprietary modems for Sega and Nintendo video game systems that online-enabled existing multi-player games.

3. In 1995 I co-founded WebTV Networks, Inc., not only conceiving of the product and designing its hardware (including architecting the central VLSI chips) and software, but acting as its President and Chief Executive Officer. While at WebTV, I created and introduced the first mass-market Internet-based consumer product: the WebTV® Internet Terminal. WebTV was a revolutionary product that combined Internet TV, and in later versions, interactive TV, digital TV, a Digital Video Recorder (DVR), and games into an integrated, simple and inexpensive consumer electronics device. A significant percentage of the hardware, software, signal processing and image processing technology was architected and designed by me personally. Twenty months after it was founded, WebTV was acquired by Microsoft Corporation for over $500 million. After the acquisition I became President of Microsoft's WebTV Division, in charge of over 700 employees internationally, developing virtually all of Microsoft's TV-related products at the time, including their digital satellite and digital cable TV products. Over 3 million WebTV

products have been sold throughout the world, and have been deployed to both DirecTV® and Dish Network® satellite customers. WebTV introduced the first DVR (three months before TiVo or ReplayTV), the first DVR for satellite TV (more than a year and more than 200,000 units before any other product was introduced), and the first DVR with two functional tuners, all based on my technology. WebTV (now sold as MSNTV) has also been quite financially successful, all based on the core software, hardware and network architecture I designed. Unlike almost all online services introduced in the dot-com era, WebTV was profitable 18 months after launch and has remained profitable every quarter since then to this day. It has produced over $1.3 billion in revenue for Microsoft. And even in 2005, ten years after founding, the base WebTV internet TV product still grossed $150 million with 65% gross margin. Furthermore, Microsoft has accrued far more value beyond this, due to the video, satellite, cable, internet media, internet protocol television, voice of internet protocol, and video game hardware technology that has grown out of the original WebTV technology.

4. I left Microsoft in 1999 to start Rearden LLC (www.rearden.com), a family of companies dedicated to the synergistic creation of art and technology. My present title is Founder and CEO of Rearden, Inc. In 2000, Rearden spun off Moxi Digital, Inc. (www.moxi.com), a company focused on revolutionizing home entertainment. At its inception, Moxi received approximately $67 million in Series 'A' funding, which remains one of the largest first-round funding dollar amounts in U.S. history for a technology start-up company. In January 2002 Moxi introduced the Moxi Media Center, a product that I created as a low-cost digital cable or satellite set-top box (STB) that integrated Digital Video Recording, Music Jukebox, DVD player, and Internet Gateway into one device that wirelessly networked video, audio, and broadband connectivity throughout the home. The Moxi Media Center was so well received in the industry that it was awarded "Best of Show" across all

categories at the 2002 Consumer Electronics Show. In May of 2002 Moxi merged with Microsoft co-founder Paul Allen's Digeo, Inc. Over 400,000 Moxi set-top boxes have been deployed by Comcast Corporation, Charter Communications, Adelphia Communications Corporation, and various other cable TV network operators.

5. Since 2002, I have founded and operated five media production and online distribution companies, all utilizing technology I have designed (OnLive, Inc. (www.onlive.com), Ice Blink Studios LLC (www.iceblink.com), MOVA LLC (www.mova.com), Rearden Studios LLC (www.reardenstudios.com), and Women of Action Media, LLC (www.woa.tv)), and I have been leading the development of advanced technologies in the areas of wireless communications, wireless power transmission, digital lenses, performance motion capture, alternative energy vehicles, and display technology, among others. I am Founder, President and CEO of OnLive, Inc., spun out from Rearden LLC in 2007, which offers video game and application on-demand services through the Internet by means of remotely hosted high-performance servers connected to homes and businesses via a proprietary low-latency video compression technology . I am Founder and President of MOVA LLC, which offers proprietary facial motion capture technology, which has been used in motion pictures such as *The Curious Case of Benjamin Button*, which won the 2008 Academy Award® for Achievement in Visual Effects for computer-generated facial aging effects. Also, I continue to consult for major corporations developing consumer electronic products as well as advise key individuals in these industries as well as in industries providing broadband media delivery, so I am very aware of the historical developments, trends and challenges that these industries have faced, as well as the present-day technological challenges.

6. During my 33-year career as an engineer and researcher I have worked with and managed hundreds of engineers, scientists, and researchers in the related fields of computers, communications (wired and wireless), entertainment, optics,

and multimedia electronics technology. I am currently named as an inventor on 81 granted U.S. patents. Products based upon these patents have produced billions of dollars in revenue. Additionally, I have designed mass-market consumer products as work for hire, or under license to me that have been sold by Apple, Microsoft, RCA, Motorola, Sony, Philips, Samsung, Panasonic, Fujitsu, Mitsubishi, Sega, Scientific Atlanta and EchoStar under their brands. These products have had to meet stringent technical and usability standards as well as extensive government and non-government agency approvals, such as those required by the FCC. Furthermore, since my work often involves pioneering new product categories, I have actively been involved in establishing US technology-related policy. For example, WebTV utilized strong encryption to prevent hacker attacks. When it was introduced, it was illegal to ship strong encryption outside of the US. Through extensive meetings with U.S. Senators, U.S. Representatives, the NSA, CIA, FBI, President Clinton and Vice President Gore and their staffs, I was successful in getting an exception to allow WebTV to be exported to Japan and the UK with strong encryption, and eventually was able to get that legislation changed to apply to all US products.

7. As a result of my extensive professional experience, I am very familiar with the skill of an ordinary practitioner working in the fields, among others, of satellite communications, wireless communications, wireless networking, video products, computer, and media-rich consumer electronic products as well, prior to 2003. I am also familiar with the skills of ordinary practitioners and the state-of-the-art in these related fields extending across the time period from 2003 to the present.

8. I am the inventor of the subject matter of the above-captioned patent application. I am familiar with the subject matter of that application and the invention defined by pending claims, as currently amended by the Amendment and Response submitted herewith. I have also read and am familiar with the prior art references

most recently cited in the above-captioned patent application, including U.S. Patent No. 6,690,657 of Lau et al. (hereinafter "Lau"); U.S. Patent No. 6,968,153 of Heinonen et al. (hereafter "Heinonen"); and U.S. Patent No. 6,115,369 of Oura (hereafter "Oura").

9. I have also read the Final Office Action dated February 18, 2009 for the above-captioned patent application and understand that claims 45-72 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lau in view of Heinonen et al. (US 6,968,153 "Heinonen") and Lau in view of Oura (US 6,115,369 "Oura")..

10. Ever since I began working on consumer electronic devices in the multimedia, communications, and entertainment industries more than 33 years ago there has existed a pressing need for a method for high-speed wireless transmission of data packets over a network without the requirements of a complex (and potentially unsightly) installation, or the limitation of having the media receiver (e.g. a television) at some fixed location where a wired connection has been installed. The advent of multi-channel television through cable TV and satellite TV services has dramatically increased the choices, features and image quality available to television viewers beyond what was available through over-the-air (OTA) terrestrial television service. Not surprisingly, cable TV and satellite TV services have come to dominate the television market, providing television service to the vast majority of US households and businesses with televisions. In almost every respect, cable TV and satellite TV service offers an improvement to consumers, but there is one significant disadvantage: the simplicity of installation, and in particular, the ability to locate the television receiver wherever it is convenient. Both cable TV and satellite TV services are typically installed by a professional installer. An appointment has to be made and usually the consumer needs to be home when the installation is done, and often it is not possible to schedule an appointment at a specific time or a convenient time, so the consumer may end up waiting around for many hours and may have to miss

work or other obligations. Then, since the installation involves thick coaxial cables that need to be snaked through walls, this often involves drilling, cutting holes in walls, and/or tacking unsightly cables onto exterior and interior walls.

11. Traditional wireless networks have worked fairly well for residential Internet traffic running at data rates below 1 megabit per second (Mbps). Audio-only transmissions for mobile telephone (cellular) networks also work well at data rates of several hundred kilobits per second (Kbps). But transmission of high-bandwidth video programs is more problematic due to the much faster video data rates. As explained in the Background section of my patent application, high-bandwidth data transmissions can be degraded by the presence of structural obstacles (e.g., walls, floors, concrete, multiple stories, etc.), large appliances (e.g., refrigerator, oven, furnace, etc.), human traffic, conflicting devices (e.g., wireless phones, microwave ovens, neighboring networks, X10 cameras, etc.), as well as by the physical distance between the access point and the mobile terminal or other device. By way of example, an IEEE 802.11b compliant wireless transceiver may have a specified data rate of 11.0 megabits per second (Mbps), but the presence of walls in the transmission path can cause the effective data rate to drop to about 1.0Mbps or less. Degradation of the video signal can also lead to repeated transmission re-tries, causing the video image to appear choppy. These practical limitations make present-day wireless technologies one of the most unreliable of all the networking options available for home media networks. There remains a substantial commercial need for a wireless repeating system that is reliable, robust (e.g. able to deal with interfering sources) and works within existing standard protocols and channel allocations.

12. The consequences of applying conventional methods of using wireless for video are quite apparent to anyone living in a multi-dwelling unit (MDU) or office building where there are many users trying to use Wi-Fi access points

simultaneously (as well as other devices, e.g. cordless phones, Bluetooth devices), all competing for the same spectrum: the connection is spotty and unreliable, particularly when users are downloading high-bandwidth data like video. The difficulties of using Wi-Fi in a multiple-user office environment were recently documented in an article entitled "Helpless, Hopeless, Wireless" published in the *Wall Street Journal* on June 26, 2007 (http://online.wsj.com/article/SB118282236794247982-search.html?KEYWORDS=wi-fi&COLLECTION=wsjie/6month). This article (a copy of which is attached as Exhibit 1) reports that the problems associated with wireless distribution of video and other media to users and customers have been so severe that the wireless market growth has slowed, despite the convenience of using wireless instead of wired connections. To quote the author (on page 3):

> Wi-Fi in offices may face further bumps, especially with the growth of new technology like online video. Since video traffic is bulkier than traditional text traffic, watching video over a wireless network can slow access speeds to a crawl and bump users off the network.

13. This *WSJ* article clearly shows that while persons of ordinary skill have been working on the problem of wireless distribution of video to remote viewers for many years, they still have failed to arrive at a practical solution. In other words, despite a long-felt need in the marketplace, others have been unable to solve the problem that I have solved with my claimed invention. This article should therefore be considered as objective evidence that the subject matter of my claims would not have been of obvious to an ordinary practitioner working at the time of my invention. This article also shows that a person of ordinary skill would recognize that there is no straightforward path or obvious approach to take in any attempt to extend distribution of real-time audiovisual content over a wireless network.

14. The claimed subject matter of the above-referenced patent application addresses the strong need for a highly reliable wireless network (e.g., on a par with

coaxial cable) that provides very high data rates (e.g., 30 Mbps) throughout the full coverage range of a home or building, and in certain embodiments, even extending well beyond the premises to reach users located an arbitrary distance away. The wireless local area network comprising a plurality of repeaters arranged in a transmission chain of my claimed invention permits data to be wirelessly transmitted at high data rates (e.g., 11Mbps or greater) to a destination device (e.g., end-user) through walls, around corners, etc., using existing protocol channel allocations (i.e., no guard bands are required), and all channels that are available can be used (i.e., there is no restriction on channel adjacency). Effectively, my claimed invention accomplishes in a practical world everything that Lau hopes to approach in an ideal world with 100% throughput and no pipeline. I explain why this is so in the paragraphs below.

15. Based on my knowledge of experience in the industry, a person of ordinary skill in the art in February 2003 – that is, someone with an engineering degree and 1-2 years experience in the field of multimedia communications – would have understood that Lau teaches a largely theoretical approach based on ideal arrangement of elements that is rarely achievable in the real world. To begin with, such a skilled practitioner would recognize that the multiple transmitters and receivers referred to in Lau are source and destination devices. This is made clear in column 5, lines 11-15, wherein he states, "T/R" devices in all of the diagrams are intended to each connect to a digital device and have a single transceiver (and they have a single antenna in the diagrams for this reason), since they are either transmitting or receiving at a given time. The repeaters, on the other hand, are receiving and transmitting constantly. This is apparent since in the figures each repeater is shown to have two antennas, meaning it has two independent RF subsystems, each for handling communications on a different frequency. Lau also makes it quite clear that the repeaters are receiving and transmitting *simultaneously*.

For example, in column 6, line 25 Lau explicitly acknowledges that it may be necessary to re-use channels and there is the risk of feedback. The reason there is the risk of feedback is because Lau is receiving and transmitting simultaneously (i.e., the same effect one hears when a public address system microphone is placed in front of its speaker: since the audio signal – or RF signal in Lau's case – is being transmitted at the same frequency at the same time it is received, the repeated transmission is picked up again by the receiver and retransmitted again, getting louder and louder, in an unending loop).

16. In my opinion, a person of ordinary skill would not consider Lau as coming close to teaching a wireless network wherein each of a plurality repeaters is arranged in a tree topology or transmission chain, with each repeater having an upstream transceiver coupled to a downstream transceiver, the upstream and downstream transceivers operating in a first frequency band, the upstream transceiver of a first repeater in the transmission chain being operable to receive data on a first channel during even time intervals, and the downstream transceiver of the first repeater being operable to transmit data at a data rate of 11Mbps or greater on the first channel to a next repeater in the transmission chain during odd time intervals, the downstream transceiver not transmitting during the even time intervals, the upstream transceiver of the next repeater receiving data during the odd time intervals, the downstream transceiver of the next repeater transmitting data at a data rate of 11Mbps or greater during the even time intervals, the downstream transceiver of the next repeater not transmitting data during the odd time intervals. Nor would a skilled artisan reading Lau with either Heinonen or Oura understand either combination as suggesting a repeater for a wireless network which includes upstream and downstream transceivers as described above together with an additional transceiver operating in a second frequency band to transmit data to at least one destination device.

17. Lau teaches are a variety of ways to establish a repeater network for which there is no compromise in network throughput. Lau lists a litany of arrangements that could be used if, in fact, an arrangement of non-interfering frequencies (or orthogonal codings, as in the case of TDMA) can be found, so that, by changing frequencies or controlling power, it is the case that the repeaters can repeat whatever the base station sends with either no interference or infrequent interference (which, in the event it occurs, would require a retransmission of data). But a person of ordinary skill would have understood that such ideal environmental arrangements are rarely available. Lau acknowledges that when simultaneously transmitting and receiving on adjacent frequencies there is a problem with a transmitter saturating a nearby receiver. (See Figure 9 and Col. 6 starting on line 53) For example, on line 58 Lau states, "The guard band allows a repeater (or T/R module) to transmit on one channel without saturating the receiver amplifier operating on the other channel, thus enabling simultaneous reception and transmission." Lau's implicit assumption in establishing guard bands is that the repeaters and T/R frequencies can be selected arbitrarily so that the guard bands can use as little spectrum as possible (e.g., Fig 9 shows a guard band that is much narrower than the spectrum for either CH1 or CH2) . Persons of skill reading Lau would understand that such flexibility is rarely the case, either in unlicensed ISM spectrum or in licensed cellular spectrum because to be compatible with existing 802.11x devices or existing cell phones, the current channel allocations must be utilized, and they generally are not allocated with guard bands. Thus, with 802.11, it would be necessary to waste an entire channel between two utilized channels, just to establish a guard band. In the 2.4 GHz band, there are only three WiFi channels, so that means using Lau this would be reduced to two WiFi channels, because the center channel required as a guard band. So, for Lau to be used at all with 2.4 GHz WiFi (which is 99% of the market for PC wireless LANs) both the 1st and 3rd

channels must be free from use by any other 2.4GHz wireless device, or Lau's entire teachings are unusable. In the 5.8GHz band there are more channels and (thus far) less public utilization, but if 1/2 of them were discarded to accommodate Lau's adjacent channel interference problem, it would be a 50% waste of spectrum.

18. Lau recognizes that such guard bands waste spectrum, but he simply sidesteps the problem and says in the next paragraph that "As more channels are added, it may be possible to decrease of eliminate the guard bands" and then describes a complex scheme that not only involves the aforementioned complexity of making sure no channel within range of another interferes very frequently with another, but adds the additional extreme complexity of having to guarantee separation between adjacent channels to avoid adjacent channel interference. For example, at column 7, lines 12-14 he says, "The pairings selected for receive and transmit channels provides the separation necessary to provide substantial non-interference." However, if Lau's teachings were used in virgin licensed spectrum and had no compatibility requirements and was not subject to any existing interference sources, such an arrangement might be conceivable. But an ordinary practitioner would have understood that back in 2003 that such arrangements are very unlikely, making Lau's scheme highly impractical.

19. An ordinary practitioner reading Lau back in 2003 would have further understood that by teaching a system that uses repeaters having transceivers that transmit and receive simultaneously on different frequency channels Lau teaches away from my claimed invention. A skilled artisan reading Lau would therefore have also been dissuaded from attempting to implement a wireless network comprising repeaters with different transceivers that transmit and receive on the same frequency channel and which receive and transmit data packets during odd/even (alternate) time intervals.

20. A person of ordinary skill in 2003 would not have understood Oura as being relevant to high data rate communications (i.e., 11Mbps or greater) because his methods are applicable only to mobile phone communication systems which have significantly lower data throughput rates (e.g., < 1 Mbps). That is also why a person of ordinary skill in the art would not consider combining Oura with Lau. Oura teaches a Time Division Multiple Access-Time Division Duplex (TDMA-TDD) communication method for transmitting and receiving between base stations and mobile phone stations. TDMA is a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA is a conventional audio communication technique that works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. Oura utilizes TDMA-TDD technology in a cellular phone network to allow a number of different users to receive forward channel signals and then, in turn, transmit reverse channel signals using the same carrier frequency.

21. In my opinion, an ordinary practitioner would not have tried to combine Oura with Lau, or modify Lau in view of Oura. One reason why is because Lau teaches away systems that utilize CSMA/CA techniques as well as TDMA services, wherein one transceiver communicates with another transceiver on a channel only when the channel is not already in use. (See column 2, line 25 through column 3 line 29) For example, Lau points out that the disadvantages of CSMA/CA and TDMA techniques include a throughput limitation of 1 Mbps, a range limitation of less than typical household dimension, bandwidth inadequate for multimedia, limitations in the number of active devices, and wasted bandwidth. By way of example, Oura discloses a data transmission speed of 384 kbps, a rate that is far too slow for reliable real-time transmission of audiovisual content at data rates of 11Mbps or greater.

22. Thus, it is my opinion that back in 2003 an ordinary practitioner would not

have had a reasonable expectation of success in combining the references in the manner suggested by the examiner in the Office Action dated February 18, 2009. For all of the reasons given above, it would have been well beyond the skill of an ordinary practitioner at the time of my invention to depart from Lau's teaching and devise a wireless network utilizing a plurality of wireless repeaters that receive and transmit in odd/even intervals as defined by my claims. It would also have been beyond the skill of an ordinary artisan to modify or combine Lau with Oura as the two references are in different fields of endeavor and, furthermore, Lau disparages the TDM approaches utilized by Oura for mobile phone communications as being unusable for high data rate (multimedia) communications.

23. Heinonen is similar to Oura in that he teaches transmission of data at low data rates. Heinonen teaches a Bluetooth repeater that may receive Bluetooth communications from an originating Bluetooth enabled device within range and then forward the same data to an intended recipient outside the range of the originating Bluetooth enabled device. At the time of my invention, a person of skill in the art would have understood that Bluetooth is a radio frequency (RF) technology with a very short effective range (e.g., 10 meters), with Bluetooth data transfers being limited to a rate of about 1 Mbps, which is far less than what is required for high-quality, high-bandwidth video transmissions. Such a person would have also understood that Bluetooth technologies are incapable of achieving data transfer rates of at least 11Mbps. Because of the enormous difference in throughput rates (and associated problems) between transmitting audio versus real-time audiovisual data, a person of ordinary skill in the art in 2003 would have dismissed Heinonen as irrelevant to the problem of wireless repeating of data at rates of 11Mbps or greater. Such an ordinary practitioner would therefore have had no reasonable expectation of success in any attempt to combine Heinonen with Lau and/or Oura to try to arrive at my claimed invention.

24. Based on my considerable experience, it is also my opinion that an ordinary practitioner would not have considered Heinonen as teaching how to use 802.11a, b or g technologies to implement a wireless network with repeaters capable of transmitting data at rates of 11Mbps or greater. Heinonen only mentions 802.11 in a single sentence at column 4, lines 10-15, which reads, preceded by two contextual sentences: "Each pair is comprised of two Bluetooth chips C1 and C2. In one embodiment, the repeater pairs 193, 193b block out all communications other than transmissions coming from the other pair. In an alternative embodiment, a portion of each repeater pair is replaced with another communications link such as, but not limited to: Bluetooth with directed antenna; cellular; IEEE 802.11a, b and g; physical links (i.e., Ethernet, twisted pair wiring, CAT 5 cabling, etc.); and/or the like." To a person of ordinary skill in the communication arts, such a configuration would limit the transmitted data rate to the data rate of the slowest link in any repeater pair. Since each repeater pair explicitly includes at least one Bluetooth chip C1 or C2, which limits the data rate of any configuration to the 1Mbps data rate of Bluetooth, this teaches away from any configuration that would support high data rate transmissions (e.g., 11Mbps) over a wireless network that includes a plurality of repeaters arranged in a transmission chain or tree topology.

25. It is my further opinion that Heinonen would have dismissed by a person of ordinary skill as largely irrelevant to a wireless network capable of transferring data at speeds associated with real-time video transmissions. Such a person would certainly have had no reasonable expectation of success at achieving my claimed invention in view of any combination of the teachings of the Lau, Oura and/or Heinonen references.

26. Heinonen also fails to teach any protocol or scheme for avoiding frequency interference so as to not compromise data throughput through the network. Rather, Heinonen's purpose is to extend the range of Bluetooth devices by use of standard

repeaters, without any concern to the impact this extension of range would have on data throughput. Given that Bluetooth was designed for low-bandwidth devices (e.g., input peripherals and audio devices) this is a reasonable trade-off since maximizing throughput is rarely a concern for Bluetooth applications. But Heinonen's approach would necessarily defeat the throughput data rate of a wireless repeater network that is attempting to approach the maximum throughput that is available in the wireless spectrum.

27. I declare, to the best of my knowledge, that all statements made in this document are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of above-captioned application or any patent issued thereon.

Date: 6/18, 2009

Stephen G. Perlman

Exhibit 1

Business Technology

Helpless, Hopeless, Wireless

Companies Cool on Hot Spots As Wi-Fi Connection Problems Lead to Help-Desk Headaches

By BOBBY WHITE

June 26, 2007; Page B1

When William Friemann joined real-estate firm Prudential Fox & Roach last year as its vice president of technology operations, he was alarmed at how much it was costing his information-technology department to continuously troubleshoot the company's patchwork wireless network.

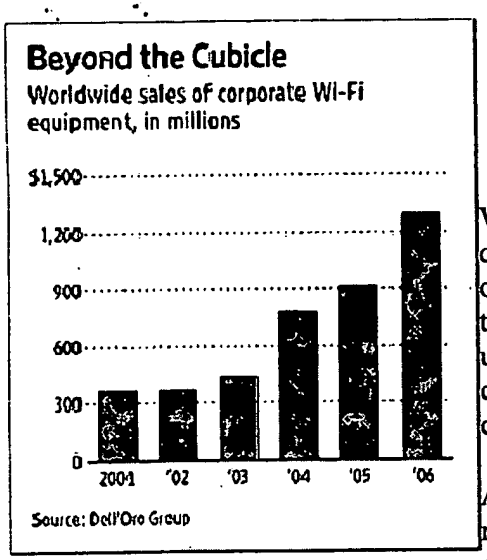
The network, which uses a wireless technology known as Wi-Fi, kicked people off if they moved away from the immediate area around a wireless access point (the antenna that receives signals from a wireless device). When employees tried to connect to the office network through a Wi-Fi connection at home, some users got bounced off the system without warning, while others were unable to make a remote connection. As a member of the help desk, Mr. Friemann often spent hours trying to solve employees' problems with the system.

Things got so bad that Mr. Friemann sometimes had employees piggyback on a neighboring business's wireless connection that was more stable -- without the other business's consent or knowledge. "It was almost like if you wanted to have remote access, you'd better expect to not have a good experience," says Mr. Friemann, 38 years old, who is based in Cherry Hill, N.J.

Wi-Fi was supposed to reduce complications, not create new ones. The wireless technology was designed to eliminate the cords and cables used to connect computers to the Internet, enabling users to be more mobile and to stay connected to the office even while on the go. Since debuting in the 1990s, the technology has been widely embraced by consumers. Wireless hot spots can now be found at many airports, hotels and **Starbucks** Corp. coffee shops.

But in many offices, Wi-Fi has been a headache. Like all radio signals, Wi-Fi is subject to interference. Its relatively low power -- less than even a typical cellphone -- means walls and cabinets can significantly reduce signal strength. Wi-Fi also creates a more open network than wired networks, raising security issues.

And Wi-Fi has caused problems for virtual private networks, or VPNs, which are lines of private communication through the public Internet created with encryption software. Some VPNs, which give users access to corporate networks from home or on the road, require a lot of processing power. If a wireless access point -- at home, at the office or on the road -- isn't robust enough, a user often gets bumped off the connection.



Wi-Fi issues have placed a great deal of stress on many corporate IT departments in part because such problems extend beyond the walls of the workplace. Many IT workers are finding that in addition to troubleshooting Wi-Fi problems at the office, they're also called upon to help when colleagues have trouble connecting to their corporate network using Wi-Fi at home, at a hotel or at a remote conference room.

All of this has stunted the growth of Wi-Fi in offices, according to research firm Dell'Oro Group. Some business users have turned away from Wi-Fi entirely. Total corporate spending on Wi-Fi equipment is still relatively small, though it's growing -- last year, companies spent $1.3 billion on Wi-Fi equipment, up from $917 million in 2005, according to Dell'Oro. In contrast, companies last year spent $16 billion on equipment that would allow them to access wired corporate networks. "Clearly there's room for growth, but there are still problems with Wi-Fi that make companies uncomfortable," says Elmer Choy, a senior analyst at Dell'Oro.

The difficulties employees have with Wi-Fi at home are often different from the troubles they face at the office. With home users, problems often occur between the configuration of their home connection and the software they have installed to access the corporate network. Sometimes the VPN software isn't compatible with the home network. At work, the main issue is often security, and how to prevent hackers and others from gaining access to the system.

Some wireless networking companies are taking steps to try to deal with customers' problems. One major issue is the stability of the wireless signal. Ruckus Wireless Inc., a wireless networking company based in Sunnyvale, Calif., tries to address that problem by providing wireless access points that have multiple antennas. That allows a Wi-Fi signal to have more than one pathway to an access point -- which can come in handy if something is in the way.

"People want Wi-Fi to do so much more," said Selina Lo, chief executive of Ruckus Wireless. "Small businesses and people at home want it to support things it hadn't in the past."

Alan Cohen, vice president of mobility solutions for **Cisco Systems** Inc., says Wi-Fi has been hurt in the office environment because the open wireless system creates problems for network administrators who are accustomed to having strict control over a network. With a Wi-Fi network, however, there is less transparency and control, he says. Still, he adds, "this is clearly a growing space."

Some advances in software and hardware have recently eased corporate users' Wi-Fi problems. Companies such as **Aruba Networks** Inc., AirTight Networks Inc. and Air Defense Inc. have new products that close security holes and alleviate problems with signal strength. AirTight, Mountain View, Calif., for instance, now makes a wireless

switch that allows a wireless network to operate like a wired network. That lets IT staffers note attempted attacks on the network and see whether unauthorized devices are attempting to connect in.

Last month, Cisco introduced new software and services that secure and extend the office Wi-Fi network to handheld devices. Some of the new services inspect incoming communications traffic for viruses and block unauthorized users from accessing the wireless network.

Adesa Inc., an auction house in Carmel, Ind., began using Wi-Fi in late 2005. But employees often brought in their own wireless equipment, creating rogue connections to the network and allowing unauthorized users to access confidential information. So last year, Chris Roberts, an Adesa network manager purchased new wireless access points with security software from AirTight; he declined to say how much he paid. After installing the equipment, he found about 173 unauthorized people using the company's wireless network. Those people could have been hackers or people downloading music or movies, which could slow down the network. The new equipment allowed Mr. Roberts to block the unapproved users.

Still, such solutions -- which can cost tens of thousands of dollars -- aren't a panacea. Since Wi-Fi operates on a similar radio frequency as other office or household devices, there tends to be more room for disruption, especially from devices that IT staffers may not originally have thought would be a problem.

That's what happened when doctors with Carilion Health Systems, a Roanoke, Va.-based health company with 100 doctor offices and eight hospitals, began using a new wireless endoscopy capsule last year. When swallowed by a patient, the capsule -- a small device about the size of a vitamin tablet -- wirelessly transmits images to a receiver as it passes through a patient's system.

Carilion's doctors were given a demo capsule early last year, but they hadn't met with the hospital's network administrators to inspect the device before they began testing it. Days later, the capsule's high-powered transmitter ended up disrupting the wireless network for the entire clinic and bumped wireless PCs and handheld scanners used by doctors and nurses off the network. Some of the devices that got knocked off the network held vital records about patients' medication dosages.

"It destroyed communication for some of our devices," says Brian Brindle, senior network engineer at Carilion. The capsule was eventually shut off after network administrators stalked the clinic halls with a Wi-Fi meter capable of detecting unauthorized wireless devices.

Wi-Fi in offices may face further bumps, especially with the growth of new technology like online video. Since video traffic is bulkier than traditional text traffic, watching video over a wireless network can slow access speeds to a crawl and bump users off the network. Last year, a new Wi-Fi standard (there are four others), dubbed 802.11n,

debuted and was supposed to solve the problem by improving signal range and download speeds. But upgrading to the new standard, which requires buying and installing new hardware and software, could prove costly for some.

For Mr. Friemann, Prudential, Fox & Roach's problems continued with the firm's wireless network until he approached managers in October and convinced them that a Wi-Fi overhaul was necessary. In January, the company began upgrading its wireless systems, spending $120,000 and tapping Aruba Wireless to help. Aruba put in a secure wireless system with high bandwidth access points that allowed the operators to better monitor who was using the network.

Today, Prudential's Wi-Fi network is more stable and Mr. Friemann's time is no longer consumed by troubleshooting. "It used to be when you walked into one of our offices and wanted wireless you had to find someone that knew what they were doing and if not, good luck, you're on your own," he says. "There's still room for improvement but what we have now is definitely better."

Write to Bobby White at bobby.white@wsj.com[1]

URL for this article:
http://online.wsj.com/article/SB118282236794247982.html

Hyperlinks in this Article:
(1) mailto:bobby.white@wsj.com

Bluetooth

From Wikipedia, the free encyclopedia

Bluetooth is an open wireless protocol for exchanging data over short distances from fixed and mobile devices, creating personal area networks (PANs). It was originally conceived as a wireless alternative to RS232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth logo.

Contents

- 1 Name and logo
- 2 Implementation
- 3 Uses
  - 3.1 Bluetooth profiles
  - 3.2 List of applications
  - 3.3 Bluetooth IEEE 802.15.1 vs. Wi-Fi IEEE 802.11 in networking
    - 3.3.1 Bluetooth devices
    - 3.3.2 Wi-Fi
- 4 Computer requirements
  - 4.1 Operating system support
- 5 Mobile phone requirements
- 6 Specifications and features
  - 6.1 Bluetooth 1.0 and 1.0B
  - 6.2 Bluetooth 1.1
  - 6.3 Bluetooth 1.2
  - 6.4 Bluetooth 2.0
  - 6.5 Bluetooth 2.1
  - 6.6 Bluetooth 3.0
  - 6.7 Bluetooth low energy
  - 6.8 Future
    - 6.8.1 UWB for AMP
- 7 Technical information
  - 7.1 Bluetooth protocol stack
    - 7.1.1 LMP (Link Management Protocol)
    - 7.1.2 L2CAP (Logical Link Control & Adaptation Protocol)
    - 7.1.3 SDP (Service Discovery Protocol)
    - 7.1.4 HCI (Host/Controller Interface)
    - 7.1.5 RFCOMM (Cable replacement protocol)
    - 7.1.6 BNEP (Bluetooth Network Encapsulation Protocol)
    - 7.1.7 AVCTP (Audio/Visual Control Transport Protocol)
    - 7.1.8 AVDTP (Audio/Visual Data Transport Protocol)

- 7.1.9 Telephone control protocol
- 7.1.10 Adopted protocols
- 7.2 Communication and connection
- 7.3 Baseband Error Correction
- 7.4 Setting up connections
- 7.5 Pairing
  - 7.5.1 Security Concerns
- 7.6 Air interface

- 8 Security
  - 8.1 Overview
  - 8.2 Bluejacking
  - 8.3 History of security concerns
    - 8.3.1 2001
    - 8.3.2 2003
    - 8.3.3 2004
    - 8.3.4 2005
    - 8.3.5 2006
    - 8.3.6 2007
- 9 Health concerns
- 10 See also
- 11 References
- 12 External links

Name and logo

The word *Bluetooth* is an anglicized version of Old Norse *Blátönn* or Danish *Blåtand*, the name of the tenth-century king Harald I of Denmark and Norway, who united dissonant Scandinavian tribes into a single kingdom. The implication is that Bluetooth does the same with communications protocols, uniting them into one universal standard.[1][2][3]

The Bluetooth logo is a bind rune merging the Germanic runes ᚼ (Hagall) and ᛒ (Berkanan).

Implementation

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 frequencies. In its basic mode, the modulation is Gaussian frequency-shift keying (GFSK). It can achieve a gross data rate of 1 Mb/s. Bluetooth provides a way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles through a secure, globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency bandwidth. The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG consists of companies in the areas of telecommunication, computing, networking, and consumer electronics.[4]

Uses

Bluetooth is a standard and communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 1 meter, 10 meters, 100 meters) based on low-cost transceiver microchips in each device.[5] Bluetooth makes it possible for these devices to communicate with each other when they are in range. Because the devices use a radio (broadcast) communications system, they do not have to be in line of sight of each other.[4]

Class	Maximum Permitted Power mW (dBm)	Range (approximate)
Class 1	100 mW (20 dBm)	~100 meters
Class 2	2.5 mW (4 dBm)	~10 meters
Class 3	1 mW (0 dBm)	~1 meter

In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to a pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

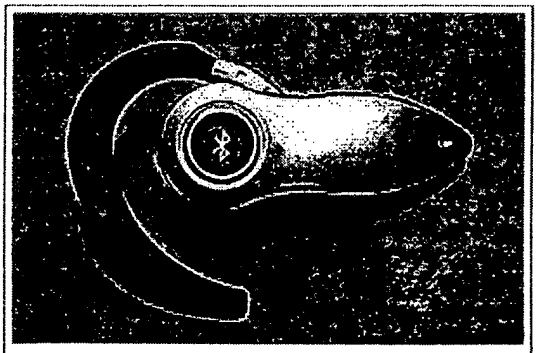
Version	Data Rate
Version 1.2	1 Mbit/s
Version 2.0 + EDR	3 Mbit/s

Bluetooth profiles

In order to use Bluetooth, a device must be compatible with certain Bluetooth profiles. These define the possible applications and uses of the technology.

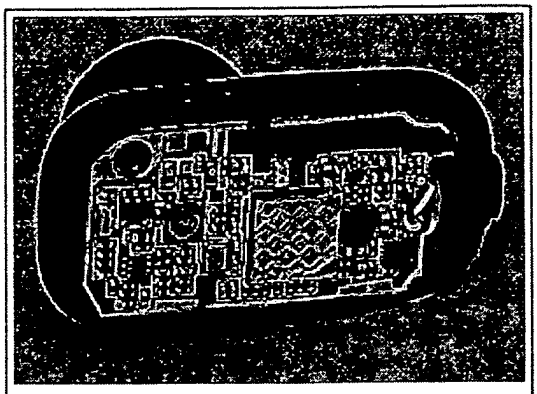
List of applications

More prevalent applications of Bluetooth include:


A typical Bluetooth mobile phone headset.

- Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used.
- For low bandwidth applications where higher [USB] bandwidth is not required and cable-free connection desired.

- Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Two seventh-generation game consoles, Nintendo's Wii[6] and Sony's PlayStation 3, use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a modem.



Nokia BH-208 headset internals.

Bluetooth IEEE 802.15.1 vs. Wi-Fi IEEE 802.11 in networking

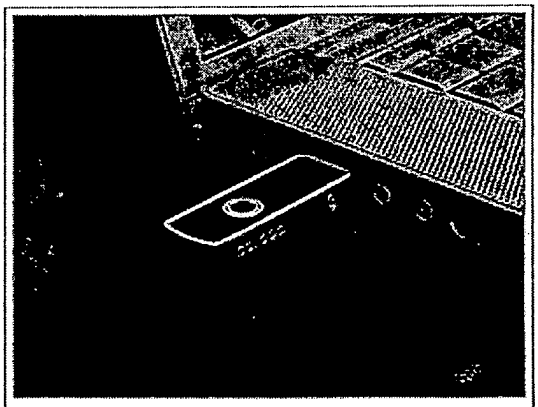
Bluetooth and Wi-Fi have many applications in today's offices, homes, and on the move: setting up networks, printing, or transferring presentations and files from PDAs to computers. Both are versions of unlicensed wireless technology.

Wi-Fi is intended for resident equipment and its applications. The category of applications is outlined as WLAN, the wireless local area networks. Wi-Fi is intended as a replacement for cabling for general local area network access in work areas.

Bluetooth is intended for non resident equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any ambience.

Bluetooth devices

Bluetooth exists in many products, such as telephones, the Wii, PlayStation 3, Lego Mindstorms NXT and recently in some high definition watches, modems and headsets. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).



A Bluetooth USB dongle with a 100 m range.

Bluetooth protocols simplify the discovery and setup of services between devices. Bluetooth devices can advertise all of the services they provide. This makes using services easier because more of the security, network address and permission configuration can be automated than with many other network types.

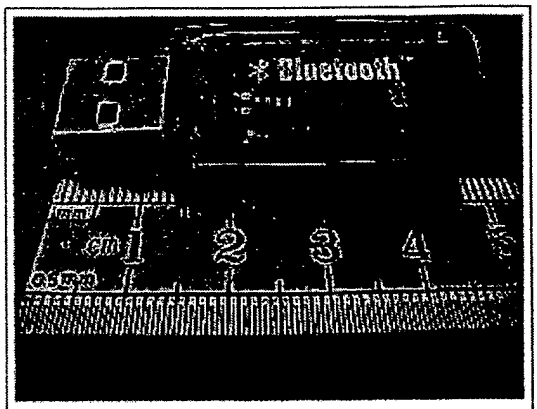
Wi-Fi

Wi-Fi is a traditional Ethernet network, and requires configuration to set up shared resources, transmit files, and to set up audio links (for example, headsets and hands-free devices). Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power, resulting in a stronger connection. Wi-Fi is sometimes called "wireless Ethernet." This description is accurate, as it also provides an indication of its relative strengths and weaknesses. Wi-Fi requires more setup but is better suited for operating full-scale

networks; it enables a faster connection, better range from the base station, and better security than Bluetooth.

Computer requirements

A personal computer must have a Bluetooth adapter in order to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recent laptops come with a built-in Bluetooth adapter, others will require an external one in the form of a dongle.



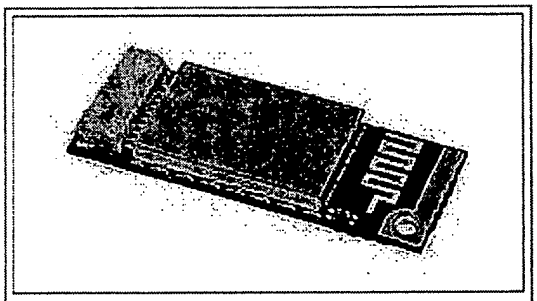
A typical Bluetooth USB dongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

Operating system support

For more details on this topic, see Bluetooth stack.

Apple has supported Bluetooth since Mac OS X v10.2 which was released in 2002.[7]


An internal notebook Bluetooth card (14×36×4 mm).

For Microsoft platforms, Windows XP Service Pack 2 and later releases have native support for Bluetooth. Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft.[8] Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at least Windows XP Service Pack 2.

Linux has two popular Bluetooth stacks, BlueZ and Affix. The BlueZ[9] stack is included with most Linux kernels and was originally developed by Qualcomm. The Affix stack was developed by Nokia. FreeBSD features Bluetooth support since its 5.0 release. NetBSD features Bluetooth support since its 4.0 release. Its Bluetooth stack has been ported to OpenBSD as well.

Mobile phone requirements

A mobile phone that is Bluetooth enabled is able to pair with many devices. To ensure the broadest support of feature functionality together with legacy device support, the Open Mobile Terminal Platform (OMTP) forum has recently published a recommendations paper, entitled "Bluetooth Local Connectivity"; see external links below to download this paper.

This publication recommends two classes, Basic and Advanced, with requirements that cover imaging, printing, stereo audio and in-car usage.

Specifications and features

The Bluetooth specification was developed in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson Mobile Platforms in Lund, Sweden.[10] The specification is based on frequency-hopping spread spectrum technology.

The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on May 20, 1998. Today it has a membership of over 11,000 companies worldwide. It was established by Ericsson, IBM, Intel, Toshiba, and Nokia, and later joined by many other companies.

Bluetooth 1.0 and 1.0B

Versions 1.0 and 1.0B had many problems, and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

Bluetooth 1.1

- Ratified as IEEE Standard 802.15.1-2002.
- Many errors found in the 1.0B specifications were fixed.
- Added support for non-encrypted channels.
- Received Signal Strength Indicator (RSSI).

Bluetooth 1.2

This version is backward compatible with 1.1 and the major enhancements include the following:

- Faster Connection and Discovery
- *Adaptive frequency-hopping spread spectrum (AFH)*, which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
- Higher transmission speeds in practice, up to 721 kbit/s, than in 1.1.
- Extended Synchronous Connections (eSCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better support for concurrent data transfer.
- Host Controller Interface (HCI) support for three-wire UART.
- Ratified as IEEE Standard 802.15.1-2005.
- Introduced Flow Control and Retransmission Modes for L2CAP.

Bluetooth 2.0

This version of the Bluetooth specification was released on November 10, 2004. It is backward compatible with the previous version 1.2. The main difference is the introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 megabits per second, although the practical data transfer rate is 2.1 megabits per second.[11] The additional throughput is obtained by using a different radio technology for transmission of the data. Standard, or Basic Rate, transmission uses Gaussian Frequency Shift Keying (GFSK) modulation of the radio signal with a gross air data rate

of 1 Mbit/s. EDR uses a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK. These have gross air data rates of 2, and 3 Mbit/s respectively. [12]

According to the 2.0 specification, EDR provides the following benefits:

- Three times faster transmission speed — up to 10 times (2.1 Mbit/s) in some cases.
- Reduced complexity of multiple simultaneous connections due to additional bandwidth.
- Lower power consumption through a reduced duty cycle.

The Bluetooth Special Interest Group (SIG) published the specification as "Bluetooth 2.0 + EDR" which implies that EDR is an optional feature. Aside from EDR, there are other minor improvements to the 2.0 specification, and products may claim compliance to "Bluetooth 2.0" without supporting the higher data rate. At least one commercial device, the HTC TyTN Pocket PC phone, states "Bluetooth 2.0 without EDR" on its data sheet.[13]

Bluetooth 2.1

Bluetooth Core Specification Version 2.1 is fully backward compatible with 1.2, and was adopted by the Bluetooth SIG on July 26, 2007.[12] This specification includes the following features:

- **Extended Inquiry Response** (EIR): provides more information during the inquiry procedure to allow better filtering of devices before connection. This information may include the name of the device, a list of services the device supports, the transmission power level used for inquiry responses, and manufacturer defined data.

- **Sniff Subrating**: reduces the power consumption when devices are in the sniff low-power mode, especially on links with asymmetric data flows. Human interface devices (HID) are expected to benefit the most, with mouse and keyboard devices increasing their battery life by a factor of 3 to 10. It lets devices decide how long they will wait before sending keepalive messages to one another. Previous Bluetooth implementations featured keep alive message frequencies of up to several times per second. In contrast, the 2.1 specification allows pairs of devices to negotiate this value between them to as infrequently as once every 5 or 10 seconds.

- **Encryption Pause Resume** (EPR): enables an encryption key to be changed with less management required by the Bluetooth host. Changing an encryption key must be done for a role switch of an encrypted an ACL link, or every 23.3 hours (one Bluetooth day) encryption is enabled on an ACL link. Before this feature was introduced, when an encryption key is refreshed the Bluetooth host would be notified of a brief gap in encryption while the new key was generated; so the Bluetooth host was required to handle pausing data transfer (however data requiring encryption may already have been sent before the notification that encryption is disabled has been received). With EPR, the Bluetooth host is not notified of the gap, and the Bluetooth controller ensures that no unencrypted data is transferred while they key is refreshed.

- **Secure Simple Pairing** (SSP): radically improves the pairing experience for Bluetooth devices, while increasing the use and strength of security. It is expected that this feature will significantly increase the use of Bluetooth.[14]

- Near Field Communication (NFC) cooperation: automatic creation of secure Bluetooth connections when NFC radio interface is also available. This functionality is part of the Secure Simple Pairing where NFC is one way of exchanging pairing information. For example, a headset should be paired with a Bluetooth 2.1 phone including NFC just by bringing the two devices close

to each other (a few centimeters). Another example is automatic uploading of photos from a mobile phone or camera to a digital picture frame just by bringing the phone or camera close to the frame.[15][16]

Bluetooth 3.0

The 3.0 specification[12] was adopted by the Bluetooth SIG (https://www.bluetooth.org/apps/content/) on April 21st, 2009. Its main new feature is AMP (Alternate MAC/PHY), the addition of 802.11 as a high speed transport. Two technologies had been anticipated for AMP: 802.11 and UWB, but UWB is missing from the specification[17].

- **Alternate MAC PHY**: enables the use of alternative MAC and PHY's for transporting Bluetooth profile data. The Bluetooth Radio is still used for device discovery, initial connection and profile configuration, however when lots of data needs to be sent, the high speed alternate MAC PHY (802.11, typically associated with Wi-Fi) will be used to transport the data. This means that the proven low power connection models of Bluetooth are used when the system is idle, and the low power per bit radios are used when lots of data needs to be sent.
- **Unicast Connectionless Data**: permits service data to be sent without establishing an explicit L2CAP channel. It is intended for use by applications that require low latency between user action and reconnection/transmission of data. This is only appropriate for small amounts of data.
- **Read Encryption Key Size**: introduces a standard HCI command for a Bluetooth host to query the encryption key size on an encrypted ACL link. The encryption key size used on a link is required for the SIM Access Profile, so generally Bluetooth controllers provided this feature in a proprietary manner. Now the information is available over the standard HCI interface.

Bluetooth low energy

On April 20, 2009, Bluetooth SIG presented the new Bluetooth low energy as an entirely additional protocol stack, compatible with other existing Bluetooth protocol stacks. The preceding naming as 'Wibree' and 'Bluetooth ULP' (Ultra Low Power) has been outdated by the final naming as 'Bluetooth low energy'.

On June 12, 2007, Nokia and Bluetooth SIG had announced that Wibree will be a part of the Bluetooth specification, as an ultra-low power Bluetooth technology.[18] Expected use cases include watches displaying Caller ID information, sports sensors monitoring your heart rate during exercise, and medical devices. The Medical Devices Working Group is also creating a medical devices profile and associated protocols to enable this market. Bluetooth low energy technology is designed for devices to have a battery life of up to one year.

Future

- **Broadcast Channel**: enables Bluetooth information points. This will drive the adoption of Bluetooth into mobile phones, and enable advertising models based around users pulling information from the information points, and not based around the object push model that is used in a limited way today.

- **Topology Management**: enables the automatic configuration of the piconet topologies especially in scatternet situations that are becoming more common today. This should all be invisible to the users of the technology, while also making the technology just work.

- QoS improvements: enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.

UWB for AMP

The high speed (AMP) feature of Bluetooth 3.0 is based on 802.11, but the AMP mechanism was designed to be usable with other radios as well. It was originally intended for UWB, but the WiMedia Alliance, the body responsible for the flavor of UWB intended for Bluetooth, announced in March 2009 that it was disbanding.

On March 16, 2009, the WiMedia Alliance announced it was entering into technology transfer agreements for the WiMedia Ultra-wideband (UWB) specifications. WiMedia will transfer all current and future specifications, including work on future high speed and power optimized implementations, to the Bluetooth Special Interest Group (SIG), Wireless USB Promoter Group and the USB Implementers Forum. After the successful completion of the technology transfer, marketing and related administrative items, the WiMedia Alliance will cease operations.[19]

Technical information

Bluetooth protocol stack

"Bluetooth is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols, and adopted protocols".[20]

Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP

Additionally, these protocols are almost universally supported: HCI and RFCOMM

LMP (Link Management Protocol)

Used for control of the radio link between two devices. Implemented on the controller.

L2CAP (Logical Link Control & Adaptation Protocol)

Used to multiplex multiple logical connections between two devices using different higher level protocols. Provides segmentation and reassembly of on-air packets.

In Basic mode, L2CAP provides packets with a payload configurable up to 64kB, with 672 bytes as the default MTU, and 48 bytes as the minimum mandatory supported MTU.

In Retransmission & Flow Control modes, L2CAP can be configured for reliable or isochronous data per channel by performing retransmissions and CRC checks.

Bluetooth Core Specification Addendum 1 adds two additional L2CAP modes to the core specification. These modes effectively deprecate original Retransmission and Flow Control modes:

- **Enhanced Retransmission Mode** (ERTM): This mode is an improved version of the original retransmission mode. This mode provides a reliable L2CAP channel.

- **Streaming Mode** (SM): This is a very simple mode, with no retransmission or flow control. This mode provides an unreliable L2CAP channel.

Reliability in any of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio will flush packets). In-order sequencing is guaranteed by the lower layer.

Only L2CAP channels configured in ERTM or SM may be operated over AMP logical links.

SDP (Service Discovery Protocol)

Used to allow devices to discover what services each other support, and what parameters to use to connect to them. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (Headset Profile, Hands Free Profile, Advanced Audio Distribution Profile etc) and the protocol multiplexer settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128)

HCI (Host/Controller Interface)

Standardised communication between the host stack (e.g. a PC or mobile phone OS) and the controller (the Bluetooth I.C.) This standard allows the host stack or controller I.C. to be swapped with minimal adaptation.

There are several HCI transport layer standards, each using a different hardware interface to transfer the same command, event and data packets. The most commonly used are USB (in PCs) and UART (in mobile phones and PDAs).

In Bluetooth devices with simple functionality, e.g. headsets, the host stack and controller can be implemented on the same microprocessor. In this case the HCI is optional, although often implemented as an internal software interface.

RFCOMM (Cable replacement protocol)

Radio frequency communications (RFCOMM) is the cable replacement protocol used to create a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

BNEP (Bluetooth Network Encapsulation Protocol)

BNEP is used to transfer another protocol stack's data via an L2CAP channel. Its main purpose is the transmission of IP packets in the Personal Area Networking Profile. BNEP performs a similar function to SNAP in Wireless LAN.

AVCTP (Audio/Visual Control Transport Protocol)

Used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player

AVDTP (Audio/Visual Data Transport Protocol)

Used by the advanced audio distribution profile to stream music to stereo headsets over an L2CAP channel. Intended to be used by video distribution profile.

Telephone control protocol

Telephony control protocol-binary (TCS BIN) is the bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices. Additionally, "TCS BIN defines mobility management procedures for handling groups of Bluetooth TCS devices"

TCS-BIN is only used by the cordless telephony profile, which failed to attract implementers. As such it is only of historical interest.

Adopted protocols

Adopted protocols are defined by other standards-making organizations and incorporated into Bluetooth's protocol stack, allowing Bluetooth to create protocols only when necessary. The adopted protocols include:

Point-to-Point Protocol (PPP) – Internet standard protocol for transporting IP datagrams over a point-to-point link

TCP/IP/UDP – Foundation Protocols for TCP/IP protocol suite

Object Exchange Protocol (OBEX) – Session-layer protocol for the exchange of objects, providing a model for object and operation representation

Wireless Application Environment / Wireless Application Protocol (WAE/WAP) – WAE specifies an application framework for wireless devices and WAP is an open standard to provide mobile users access to telephony and information services.[20]

Communication and connection

A master Bluetooth device can communicate with up to seven devices in a Wireless User Group. This network group of up to eight devices is called a piconet.

A piconet is an ad-hoc computer network, using Bluetooth technology protocols to allow one master device to interconnect with up to seven active devices. Up to 255 further devices can be inactive, or parked, which the master device can bring into active status at any time.

At any given time, data can be transferred between the master and one other device, however, the devices can switch roles and the slave can become the master at any time. The master switches rapidly from one device to another in a round-robin fashion. (Simultaneous transmission from the master to multiple other devices is possible, but not used much.)

The Bluetooth specification allows connecting two or more piconets together to form a scatternet, with some devices acting as a bridge by simultaneously playing the master role in one piconet and the slave role in another.

Many USB Bluetooth adapters are available, some of which also include an IrDA adapter. Older (pre-2003) Bluetooth adapters, however, have limited services, offering only the Bluetooth Enumerator and a less-powerful Bluetooth Radio incarnation. Such devices can link computers with Bluetooth, but they do not offer much in the way of services that modern adapters do.

Baseband Error Correction

Three types of error correction are implemented in Bluetooth systems,

- 1/3 rate (Forward Error Correction) (FEC)
- 2/3 rate FEC
- Automatic Repeat Request (ARQ)

Setting up connections

Any Bluetooth device will transmit the following information on demand:

- Device name.
- Device class.
- List of services.
- Technical information, for example, device features, manufacturer, Bluetooth specification used, clock offset.

Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of a device's services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops show only the Bluetooth names and special programs are required to get additional

information about remote devices. This can be confusing as, for example, there could be several phones in range named T610 (see Bluejacking).

Pairing

Pairs of devices may establish a relationship by creating a shared secret known as a *link key*, this process is known as *pairing*. If a link key is stored by both devices they are said to be *bonded*. A device that wants to communicate only with a bonded device can cryptographically authenticate the identity of the other device, and so be sure that it is the same device it previously paired with. Once a link key has been generated, an authenticated ACL link between the devices may be encrypted so that the data that they exchange over the airwaves is protected against eavesdropping. Link keys can be deleted at any time by either device, if done by either device this will implicitly remove the bonding between the devices; so it is possible one of the device to have a link key stored but not be aware that it is no longer bonded to the device associated with the given link key.

Bluetooth services generally require either encryption or authentication, as such require pairing before they allow a remote device to use the given service. Some services, such as the Object Push Profile, elect not to explicitly require authentication or encryption so that pairing does not interfere with the user experience associated with the service use-cases.

Pairing mechanisms have changed significantly with the introduction of Secure Simple Pairing in Bluetooth 2.1. The following summarizes the pairing mechanisms:

- **Legacy pairing**: This is the only method available before Bluetooth 2.1. Each device must enter a PIN code, pairing is only successful if both devices enter the same PIN code. Any 16-digit ACSII string may be used as a PIN code, however not all devices may be capable of entering all possible PIN codes.
  - **Limited Input Devices**: The obvious example of this class of device is a Bluetooth Hands-free headset, which generally have few inputs. These devices usually have a *fixed PIN*, for example "0000" or "1234", that are hard-coded into the device.
  - **Numeric Input Devices**: Mobile phones are classic examples of these devices. They allow a user to enter a numeric value up-to 16 digits in length.
  - **Alpha-numeric Input Devices**: PCs and smartphones are examples of these devices. They allow a user to enter full ASCII text as a PIN code. If pairing with a less capable device the user needs to be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may use.
- **Secure Simple Pairing**: This is required by Bluetooth 2.1. A Bluetooth 2.1 device may only use legacy pairing to interoperable with a 2.0 or older device. Secure Simple Pairing uses a type of public key cryptography, and has the following modes of operation:
  - **Just Works**: As implied by the name, this method just works. No user interaction is required; however, a device may prompt the user to confirm the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN mechanism which is typical for this set of limited devices. This method provides no man in the middle (MITM) protection.
  - **Numeric Comparison**: If both devices have a display and at least one can accept a binary Yes/No user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user should compare the numbers to insure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, assuming the user confirms on both devices and actually performs the comparison properly.

- **Passkey Entry**: This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both cases provide MITM protection.
- **Out of Band** (OOB): This method uses an external means of communication (such as NFC) to exchange some information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. This method provides some level of MITM protection, assuming the OOB method used provides MITM.

SSP is considered simple for the following reasons:

- In most cases it does not require a user to generate a passkey.
- For use-cases not requiring MITM, user interaction has been eliminated.
- For Numeric Comparison, MITM protection can be achieved with a simple Yes/No decision by the user.
- Using OOB with NFC will enable pairing when devices simply get close, rather than requiring a lengthy discovery process.

Security Concerns

Prior to Bluetooth 2.1, encryption is not required and can be turned off at any time. Moreover, the encryption key is only good for approximately 23.5 hours; using a single encryption key longer than this time allows simple XOR attacks to retrieve the encryption key.

- Turning off encryption is required for several normal operations, so it is problematic to detect if encryption is disabled for a valid reason or for a security attack.
- Bluetooth 2.1 addresses this in the following ways:
  - Encryption is required for all non SDP (Service Discovery Protocol) connections
  - A new Encryption Pause and Resume feature is used for all normal operations requiring encryption to be disabled. This enables easy identification of normal operation from security attacks.
  - The encryption key is required to be refreshed before it expires.

Link keys may be stored on the device file system, not on the Bluetooth chip itself. Many Bluetooh chip manufacturers allow link keys to be stored on the device; however, if the device is removable this means that the link key will move with the device.

Air interface

The protocol operates in the license-free ISM band at 2.4-2.4835 GHz. To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels up to 1600 times per second. Implementations with versions 1.1 and 1.2 reach speeds of 723.1 kbit/s. Version 2.0 implementations feature Bluetooth Enhanced Data Rate (EDR) and reach 2.1 Mbit/s. Technically, version 2.0 devices have a higher power consumption, but the three times faster rate reduces the transmission times, effectively reducing power consumption to half that of 1.x devices (assuming equal traffic load).

Security

Overview

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. In Bluetooth, key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN, e.g. for headsets or similar devices with a restricted user interface. During pairing, an initialization key or master key is generated, using the E22 algorithm.[21] The E0 stream cipher is used for encrypting packets, granting confidentiality and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

An overview of Bluetooth vulnerabilities exploits has been published by Andreas Becker.[22]

In September 2008, the National Institute of Standards and Technology (NIST) published a Guide to Bluetooth Security that will serve as reference to organization on the security capabilities of Bluetooth and steps for securing Bluetooth technologies effectively. While Bluetooth has its benefits, it is susceptible to denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Users/organizations must evaluate their acceptable level of risk and incorporate security into the lifecycle of Bluetooth devices. To help mitigate risks, included in the NIST document are security checklists with guidelines and recommendations for creating and maintaining secure Bluetooth piconets, headsets, and smart card readers.[23]

Bluejacking

Bluejacking is the sending of either a picture or a message from one user to an unsuspecting user through Bluetooth wireless technology. Common applications are short messages (e.g., "You've just been bluejacked!"), advertisements (e.g., "Eat at Joe's"), and business information.[24] Bluejacking does not involve the removal or alteration of any data from the device.

History of security concerns

2001

In 2001, Jakobsson and Wetzel from Bell Laboratories discovered flaws in the pairing protocol of Bluetooth, and also pointed to vulnerabilities in the encryption scheme. [25]

2003

In November 2003, Ben and Adam Laurie from A.L. Digital Ltd. discovered that serious flaws in Bluetooth security may lead to disclosure of personal data.[26] It should be noted, however, that the reported security problems concerned some poor implementations of Bluetooth, rather than the protocol itself.

In a subsequent experiment, Martin Herfurt from the trifinite.group was able to do a field-trial at the CeBIT fairgrounds, showing the importance of the problem to the world. A new attack called BlueBug was used for this experiment.[27] This is one of a number of concerns that have been raised over the security of Bluetooth communications.

2004

In 2004 the first purported virus using Bluetooth to spread itself among mobile phones appeared on the Symbian OS.[28] The virus was first described by Kaspersky Lab and requires users to confirm the installation of unknown software before it can propagate. The virus was written as a proof-of-concept by a group of virus writers known as "29A" and sent to anti-virus groups. Thus, it should be regarded as a potential (but not real) security threat to Bluetooth or Symbian OS since the virus has never spread outside of this system.

In August 2004, a world-record-setting experiment (see also Bluetooth sniping) showed that the range of Class 2 Bluetooth radios could be extended to 1.78 km (1.08 mile) with directional antennas and signal amplifiers.[29] This poses a potential security threat because it enables attackers to access vulnerable Bluetooth-devices from a distance beyond expectation. The attacker must also be able to receive information from the victim to set up a connection. No attack can be made against a Bluetooth device unless the attacker knows its Bluetooth address and which channels to transmit on.

2005

In January 2005, a mobile malware worm known as Lasco.A began targeting mobile phones using Symbian OS (Series 60 platform) using Bluetooth-enabled devices to replicate itself and spread to other devices. The worm is self-installing and begins once the mobile user approves the transfer of the file (velasco.sis) from another device. Once installed, the worm begins looking for other Bluetooth-enabled devices to infect. Additionally, the worm infects other .SIS files on the device, allowing replication to another device through use of removable media (Secure Digital, Compact Flash, etc.). The worm can render the mobile device unstable.[30]

In April 2005, Cambridge University security researchers published results of their actual implementation of passive attacks against the PIN-based pairing between commercial Bluetooth devices, confirming the attacks to be practicably fast and the Bluetooth symmetric key establishment method to be vulnerable. To rectify this vulnerability, they carried out an implementation which showed that stronger, asymmetric key establishment is feasible for certain classes of devices, such as mobile phones.[31]

In June 2005, Yaniv Shaked (http://www.eng.tau.ac.il/~shakedy) and Avishai Wool (http://www.eng.tau.ac.il/~yash/) published a paper describing both passive and active methods for obtaining the PIN for a Bluetooth link. The passive attack allows a suitably equipped attacker to eavesdrop on communications and spoof, if the attacker was present at the time of initial pairing. The active method makes use of a specially constructed message that must be inserted at a specific point in the protocol, to make the master and slave repeat the pairing process. After that, the first method can be used to crack the PIN. This attack's major weakness is that it requires the user of the devices under attack to re-enter the PIN during the attack when the device prompts them to. Also, this active attack probably requires custom hardware, since most commercially available Bluetooth devices are not capable of the timing necessary.[32]

In August 2005, police in Cambridgeshire, England, issued warnings about thieves using Bluetooth-enabled phones to track other devices left in cars. Police are advising users to ensure that any mobile networking connections are de-activated if laptops and other devices are left in this way.[33]

2006

In April 2006, researchers from Secure Network and F-Secure published a report that warns of the large number of devices left in a visible state, and issued statistics on the spread of various Bluetooth services and the ease of spread of an eventual Bluetooth worm.[34]

2007

In October 2007, at the Luxemburgish Hack.lu Security Conference, Kevin Finistere and Thierry Zoller demonstrated and released a remote root shell via Bluetooth on Mac OS X v10.3.9 and v10.4. They also demonstrated the first Bluetooth PIN and Linkkeys cracker, which is based on the research of Wool and Shaked.

Health concerns

Bluetooth uses the microwave radio frequency spectrum in the 2.4 GHz to 2.4835 GHz range. Maximum power output from a Bluetooth radio is 100 mW, 2.5 mW, and 1 mW for Class 1, Class 2, and Class 3 devices respectively, which puts Class 1 at roughly the same level as mobile phones, and the other two classes much lower.[35] Accordingly, Class 2 and Class 3 Bluetooth devices are considered less of a potential hazard than mobile phones, and Class 1 may be comparable to that of mobile phones.

See also

- Bluejacking
- Bluesniping
- Java APIs for Bluetooth
- Jellingspot Data Server
- Handsfree
- IEEE 802.15
- List of computer standards
- Near Field Communication
- Personal Area Network
- Tethering
- Wibree - complementary standard with lower power consumption, developed by Nokia, now named ULP Bluetooth.
- Wireless USB
- ZigBee - low power lightweight wireless protocol in the ISM band.

References

1. ^ Monson, Heidi (1999-12-14). "Bluetooth Technology and Implications". SysOpt.com. http://www.sysopt.com/features/network/article.php/3532506. Retrieved on 2009-02-17.
2. ^ "About the Bluetooth SIG". Bluetooth SIG. http://www.bluetooth.com/Bluetooth/SIG/. Retrieved on 2008-02-01.
3. ^ Kardach, Jim (2008-05-03). "How Bluetooth got its name". http://www.eetimes.eu/scandinavia/206902019?cid=RSSfeed_eetimesEU_scandinavia. Retrieved on 2009-02-24.
4. ^ [a] [b] Newton, Harold. (2007). *Newton's telecom dictionary.* New York: Flatiron Publishing.

5. ^ "How Bluetooth Technology Works". Bluetooth SIG. http://www.bluetooth.com/Bluetooth/Technology/Works/. Retrieved on 2008-02-01.
6. ^ "Wii Controller". Bluetooth SIG. http://bluetooth.com/Bluetooth/Products/Products/Product_Details.htm?ProductID=2951. Retrieved on 2008-02-01.
7. ^ Apple (2002-07-17). *Apple Introduces "Jaguar," the Next Major Release of Mac OS X.* Press release. http://www.apple.com/pr/library/2002/jul/17jaguar.html. Retrieved on 2008-02-04.
8. ^ "Network Protection Technologie". *Changes to Functionality in Microsoft Windows XP Service Pack 2.* Microsoft Technet. http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx. Retrieved on 2008-02-01.
9. ^ BlueZ - Official Linux Bluetooth protocol stack (http://www.bluez.org)
10. ^ "The Bluetooth Blues". Information Age. 2001-05-24. http://www.information-age.com/article/2001/may/the_bluetooth_blues. Retrieved on 2008-02-01.
11. ^ Guy Kewney (2004-11-16). "High speed Bluetooth comes a step closer: enhanced data rate approved". Newswireless.net. http://www.newswireless.net/index.cfm/article/629. Retrieved on 2008-02-04.
12. ^ [a] [b] [c] "Specification Documents". Bluetooth SIG. http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/. Retrieved on 2008-02-04.
13. ^ "HTC TyTN Specification" (PDF). HTC. http://www.europe.htc.com/z/pdf/products/1766_TyTN_LFLT_OUT.PDF. Retrieved on 2008-02-04.
14. ^ (PDF) *Simple Pairing Whitepaper*. Version V10r00. Bluetooth SIG. 2006-08-03. http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf. Retrieved on 2007-02-01.
15. ^ Michael Oryl (2007-03-15). "Bluetooth 2.1 Offers Touch Based Pairing, Reduced Power Consumption". MobileBurn. http://www.mobileburn.com/news.jsp?Id=3213. Retrieved on 2008-02-04.
16. ^ Taoufik Ghanname (2007-02-14). "How NFC can to speed Bluetooth transactions-today". Wireless Net DesignLine. http://www.wirelessnetdesignline.com/howto/showArticle.jhtml?articleID=180201430. Retrieved on 2008-02-04.
17. ^ David Meyer (2009-04-22). "Bluetooth 3.0 released without ultrawideband". zdnet.co.uk. http://news.zdnet.co.uk/communications/0,1000000085,39643174,00.htm. Retrieved on 2009-04-22.
18. ^ Nokia (2007-06-12) (PDF). *Wibree forum merges with Bluetooth SIG*. Press release. http://www.wibree.com/press/Wibree_pressrelease_final_1206.pdf. Retrieved on 2008-02-04.
19. ^ [1] (http://www.wimedia.org/) , [2] (http://www.wimedia.org/imwp/download.asp?ContentID=15508) , [3] (http://www.wimedia.org/imwp/download.asp?ContentID=15506) , [4] (http://www.bluetooth.com/Bluetooth/Technology/Technology_Transfer/) , [5] (http://www.usb.org/press/WiMedia_Tech_Transfer/) , [6] (http://www.incisor.tv/2009/03/what-to-make-of-bluetooth-sig-wimedia.html)
20. ^ [a] [b] Stallings, William. (2005). *Wireless communications & networks.* Upper Saddle River, NJ: Pearson Prentice Hall.
21. ^ Juha T. Vainio (2000-05-25). "Bluetooth Security". Helsinki University of Technology. http://www.iki.fi/jiitv/bluesec.pdf. Retrieved on 2009-01-01.
22. ^ Andreas Becker (2007-08-16) (PDF). *Bluetooth Security & Hacks*. Ruhr-Universität Bochum. http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf. Retrieved on 2007-10-10.
23. ^ Scarfone, K., and Padgette, J. (September 2008) (PDF). *Guide to Bluetooth Security*. National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf. Retrieved on 2008-10-03.
24. ^ "What is bluejacking?". Helsinki University of Technology. http://www.bluejackq.com/what-is-bluejacking.shtml. Retrieved on 2008-05-01.
25. ^ "Security Weaknesses in Bluetooth". RSA Security Conf. – Cryptographer's Track. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.7357. Retrieved on 2009-03-01.
26. ^ "Bluetooth". The Bunker. http://www.thebunker.net/resources/bluetooth. Retrieved on 2007-02-01.
27. ^ "BlueBug". Trifinite.org. http://trifinite.org/trifinite_stuff_bluebug.html. Retrieved on 2007-02-01.
28. ^ John Oates (2004-06-15). "Virus attacks mobiles via Bluetooth". The Register. http://www.theregister.co.uk/2004/06/15/symbian_virus/. Retrieved on 2007-02-01.
29. ^ "Long Distance Snarf". Trifinite.org. http://trifinite.org/trifinite_stuff_lds.html. Retrieved on 2007-02-01.
30. ^ "F-Secure Malware Information Pages: Lasco.A". F-Secure.com. http://www.f-secure.com/v-descs/lasco_a.shtml. Retrieved on 2008-05-05.

31. ^ Ford-Long Wong, Frank Stajano, Jolyon Clulow (2005-04) (PDF). *Repairing the Bluetooth pairing protocol*. University of Cambridge Computer Laboratory. http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf. Retrieved on 2007-02-01.
32. ^ Yaniv Shaked, Avishai Wool (2005-05-02). *Cracking the Bluetooth PIN*. School of Electrical Engineering Systems, Tel Aviv University. http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/. Retrieved on 2007-02-01.
33. ^ "Phone pirates in seek and steal mission". Cambridge Evening News. Archived from the original on 2007-07-17. http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf. Retrieved on 2008-02-04.
34. ^ (PDF) *Going Around with Bluetooth in Full Safety*. F-Secure. 2006-05. http://www.securenetwork.it/bluebag_brochure.pdf. Retrieved on 2008-02-04.
35. ^ M. Hietanen, T. Alanko (2005-10). "Occupational Exposure Related to Radiofrequency Fields from Wireless Communication Systems" (PDF). *XXVIIIth General Assembly of URSI - Proceedings*. Union Radio-Scientifique Internationale. http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf. Retrieved on 2007-04-19.

External links

- Bluetooth Special Interest Group Site (includes specifications) (http://www.bluetooth.org)
- Official Bluetooth site aimed at users (http://www.bluetooth.com)
- Official Bluetooth gadget guide, aimed at users (http://gadgetguide.bluetooth.com)
- OMTP Bluetooth Local Connectivity Paper (http://www.omtp.org/Publications/Display.aspx?Id=8f152a02-4120-4933-a1e5-74c7ad472bc8)
- Bluetooth affect other 3G & IMT-2000 (aka WiMAX devices) (http://news.softpedia.com/news/Bluetooth-over-Wi-Fi-Kills-Nearby-WiMax-Networks-81415.shtml) , Softpedia Report

Internet access								
Network type	Wired					Wireless		
	Optical	Coaxial cable	Ethernet cable	Phone line	Power line	Unlicensed terrestrial bands	Licensed terrestrial bands	Satellite
LAN	1000BASE-X	G.hn	Ethernet	HomePNA · G.hn	G.hn	Wi-Fi · **Bluetooth** · DECT · Wireless USB		
WAN	PON	DOCSIS		Dial-up · ISDN · DSL	BPL	Muni Wi-Fi	GPRS · iBurst · WiBro/WiMAX · UMTS-TDD, HSPA · EVDO · LTE	Satellite